3. Protección de Datos

2. Secuestro de Sesiones

2.1 Introducción

Un secuestro de sesiones se da cuando un atacante logra colocarse entre dos máquinas, y apoderarse de la sesión establecida entre ambas. Los atacantes pueden hacerse de nuestras cuentas capturando las contraseñas que viajan por la red, tanto en texto plano como encriptadas, la comunicación sucede en tiempos diferidos. De esta forma, el cliente envía una petición, el servidor la recibe y envía una respuesta con las cabeceras HTTP.

Un secuestro de sesiones es una técnica que consiste en interceptar una sesión iniciada entre dos equipos para secuestrarla. Como la comprobación de autentificación se hace sólo al abrir la sesión, un pirata que inicie su ataque con éxito puede controlar la conexión durante toda la sesión.

La inadecuada gestión de sesiones en aplicaciones web empresariales se ha convertido en la tercera vulnerabilidad en aplicaciones web. El impacto de explotar esta vulnerabilidad es crítico debido a la exposición de información restringida para el negocio.

2.2 Funcionamiento de un Secuestro de Sesiones

Un secuestro de sesión es cuando un atacante toma el control de una sesión de usuario después de que el usuario se haya autenticado correctamente con un servidor. El secuestro de sesión implica un ataque para identificar los IDs de sesión actual de una comunicación cliente/servidor y hacerse cargo de la sesión del cliente.

El secuestro de sesión es posible gracias a herramientas que realizan la predicción del número de secuencia. Los detalles de la predicción del número de secuencia se discutirán más adelante en este capítulo en la sección correspondiente.

Los ataques de suplantación de identidad son diferentes de los ataques de secuestro. En un ataque de suplantación, el atacante realiza sniffing y escucha el tráfico cuando pasa a lo largo de la red del emisor al receptor. El atacante utiliza la información recopilada para suplantar o utiliza una dirección de un sistema legítimo. El secuestro implica tomar activamente la conexión de otro usuario. El atacante se basa en el usuario legítimo para hacer una conexión y la autenticación. Después de eso, el atacante se hace cargo de la sesión y la sesión del usuario válido se desconecta.

Un secuestro de sesión implica los siguientes tres pasos para llevar a cabo un ataque:

1. Seguimiento de la Sesión: El atacante identifica una sesión abierta y predice el número de secuencia del siguiente paquete.
2. Desincronizar la conexión: El atacante envía al sistema del usuario válido un restablecimiento TCP (RST) o final (FIN) de paquetes para hacer que se cierre la sesión.
3. Inyección de paquetes: El atacante envía al servidor un paquete TCP con el número de secuencia prevista, y el servidor lo acepta como próximo paquete de usuario válido.

Los atacantes pueden usar dos tipos de secuestro de sesión: activo y pasivo. La principal diferencia entre el secuestro activo y pasivo es el nivel de participación del atacante en la sesión.

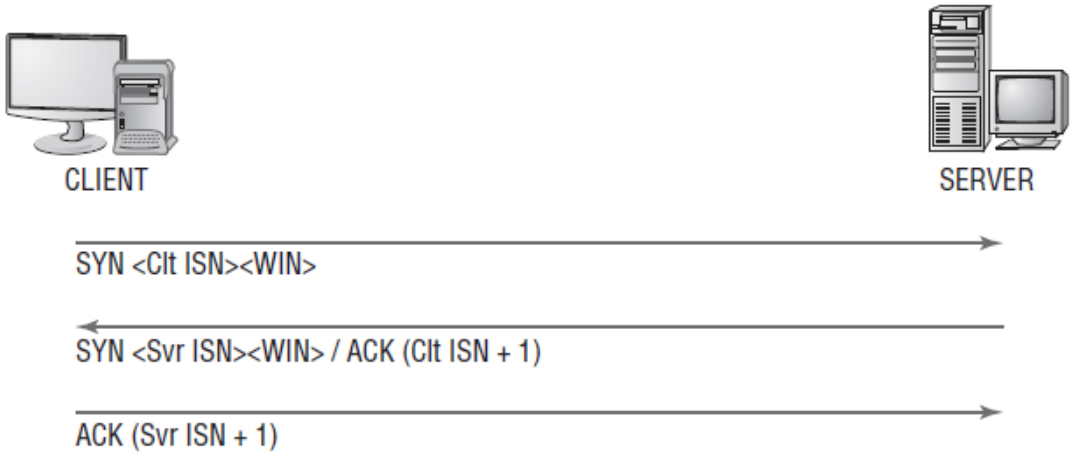
En un ataque activo, un atacante encuentra una sesión activa y se hace cargo de la sesión mediante el uso de herramientas que predicen el siguiente número de secuencia utilizado en la sesión TCP.

En un ataque pasivo, el intruso secuestra una sesión y luego observa y registra todo el tráfico que enviado por el usuario legítimo. El secuestro de sesión pasivo no es más que esnifar. Reúne información como contraseñas y luego utiliza esa información para autenticarse como una sesión independiente.

2.3 Predicción de Secuencia

TCP es un protocolo orientado a conexión responsable de volver a ensamblar flujos de paquetes en su orden original. Cada paquete tiene que tener asignado un número de sesión único que permite a la máquina receptora volver a montar el flujo de paquetes en su orden original; este número único se conoce como un número de secuencia. Si los paquetes llegan fuera de orden, como sucede con regularidad a través de Internet, el SN se utiliza para ensamblar los paquetes correctamente. Como se acaba de ilustrar, el sistema iniciando una sesión TCP transmite un paquete con el bit SYN a 1. Esto se llama un paquete de sincronización e incluye el ISN del cliente. El ISN es un número generado de forma pseudo-aleatoria, con más de 4 mil millones de combinaciones posibles, sin embargo, es estadísticamente posible que se repita.

Cuando se envía el paquete ACK, cada máquina utiliza el SN del paquete de para el que se está acusando recibo, más un incremento. Esto no sólo confirma correctamente la recepción de un paquete específico, sino también indica al emisor el siguiente SN esperado. Dentro del acuerdo de tres vías, el valor de incremento es 1. En las comunicaciones de datos normales, el valor de incremento es igual al tamaño de los datos en bytes (por ejemplo, si transmite 45 bytes de datos, el ACK responde usando el SN del paquete entrante más 45).



Las herramientas de hacking utilizadas para llevar a cabo el secuestro de sesiones hacen predicción de número de secuencia. Para llevar a cabo con éxito un ataque de predicción de secuencia TCP, el atacante debe interceptar el tráfico entre los dos sistemas. A continuación, el atacante o la herramienta de hacking deben adivinar correctamente el SN o localizar un ISN para calcular el siguiente número de secuencia. Este proceso puede ser más difícil de lo que parece, porque los paquetes viajan muy rápido.

Cuando el atacante no es capaz de esnifar la conexión, se vuelve mucho más difícil adivinar el próximo SN. Por esta razón, la mayoría de las herramientas de secuestro de sesión incluyen características para permitir el esnifado de los paquetes para determinar los SNs.

Los atacantes generan paquetes utilizando una dirección IP simulada del sistema que tenía una sesión con el sistema de destino. Las herramientas de hacking emiten paquetes con los SNs que el sistema de destino está esperando.

Pero los paquetes de los atacantes deben llegar antes que los paquetes del sistema de confianza cuya conexión está siendo secuestrada. Esto se logra por la inundación del sistema de confianza con paquetes o el envío de un paquete RST para el sistema de confianza de modo que no esté disponible para enviar paquetes al sistema de destino.

2.4 Peligros del Secuestro de Sesión

El secuestro de sesión TCP es un ataque peligroso: la mayoría de los sistemas son vulnerables debido a que utilizan TCP/IP como protocolo de comunicación principal. Los sistemas operativos más recientes han tratado de protegerse a sí mismos del secuestro de sesión mediante el uso de generadores de números pseudo-aleatorios para calcular el ISN, por lo que el número de secuencia es más difícil de adivinar. Sin embargo, esta medida de seguridad no es efectiva si el atacante es capaz de esnifar los paquetes, lo que da toda la información necesaria para llevar a cabo este ataque.

Las siguientes son las razones por las que es importante estar al tanto del secuestro de sesión:

- La mayoría de los sistemas son vulnerables.
- Hay pocas medidas disponibles para protegerse adecuadamente.
- Los ataques de secuestro de sesión son fáciles de poner en marcha.
- El secuestro es peligroso debido a la información que se puede obtener durante el ataque.